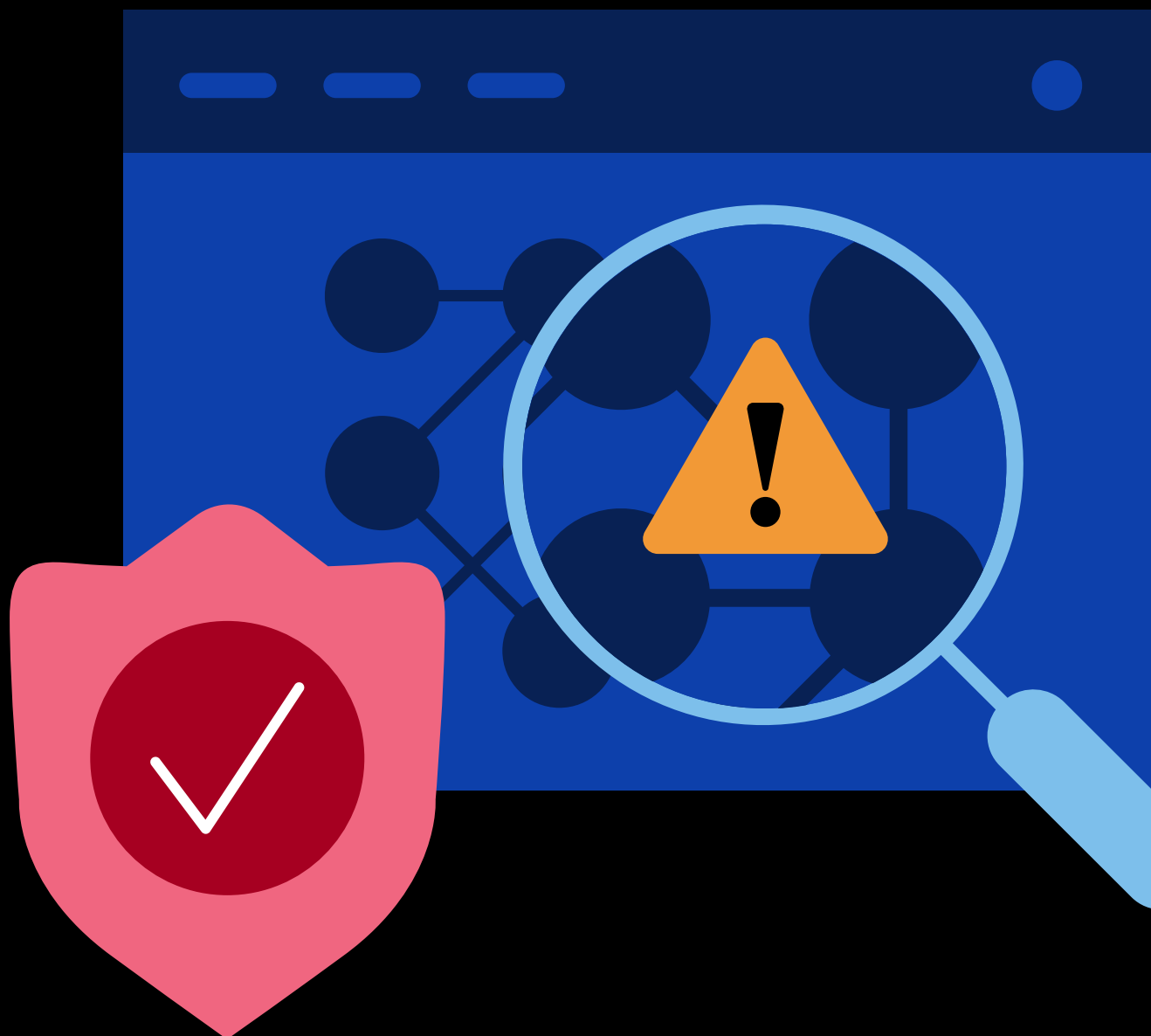




F5 Distributed Cloud Web App Scanning

Automate security reconnaissance and penetration testing for complex, modern web apps and receive actionable guidance to swiftly remediate problems.



Key benefits

Quick setup, maximum protection

Initiate scans in mere minutes; requires limited configuration and experience to get started and runs automatically.

Ensure comprehensive coverage and visibility

Work seamlessly with all types of web apps, thoroughly crawling, navigating, scanning, and testing regardless of the underlying technology.

Gain data-driven insights and remediation recommendations

Get clear and contextualized reporting, complete with screenshots, videos, and technical details, enabling a thorough understanding of findings for prompt and informed action.

Reduce threat surface and prevent data loss

Automate scanning and testing for in-depth, scalable evaluation of your web apps, enhancing visibility into vulnerabilities and sensitive data exposure.

Achieve compliance peace of mind

Leverage detailed reports and insights, facilitating compliance validation and documentation for prominent industry frameworks such as SOC 2 and ISO 27001.

Running manual penetration tests on large, distributed app portfolios is impractical and costly.

Change is constant for applications today in the dynamic world of digital transformation.

Organizations continue to modernize legacy apps and embrace new development paradigms. Emerging apps harness microservices-based architectures, becoming more distributed and undergoing frequent updates to meet the rising demands of app usage, to deliver improved performance, and to drive competitive innovation.

Navigating this complex ecosystem can tax organizations as they seek to maintain consistent visibility, control, and security, just as development models and app architectures further evolve to include multi-cloud and hybrid deployments. The proliferation of APIs and expansion of workloads beyond the cloud to the branches or customer edges accentuate the need for swift data access and critical telemetry.

Amid this shifting landscape, the task of identifying and managing threats and risks is more complex than ever. Finding and managing vulnerabilities is a full-time, arduous job, not meant to be done manually. Continuously conducting manual penetration tests on large, distributed app portfolios is impractical because of its devouring of resources and money.

The benefits of automated reconnaissance and penetration testing

Organizations must be able to seamlessly and continuously scan their entire application portfolio to reveal critical infrastructure components, web-facing services, and endpoints—and test them for vulnerabilities and data exposure risks.

With [F5® Distributed Cloud Web App Scanning](#), this daunting task becomes extremely manageable. Distributed Cloud Web App Scanning automates the scanning of the Internet, public source repositories, exposed servers, and other sources to provide a comprehensive overview of an organization's external-facing app ecosystem often susceptible to risks. After identifying exposed data and potential vulnerabilities, the F5 solution helps maintain an enhanced security posture and provides remediation guidance for immediate follow-up.

Distributed Cloud Web App Scanning continuously scans your external-facing app ecosystem, uncovering vulnerabilities while providing remediation guidance.

External attack surface management

Gain a panoramic view of your organization’s external attack surface. Distributed Cloud Web App Scanning automatically scans your domain(s) to find services and endpoints exposed online. It captures server versions, operating systems, and hosting providers across your domain(s) and pinpoints web servers compromised by known vulnerabilities (CVEs). Additionally, it offers the capability to virtually patch vulnerabilities using the Web App and API Protection (WAAP) features included in [F5 Distributed Cloud Services](#).

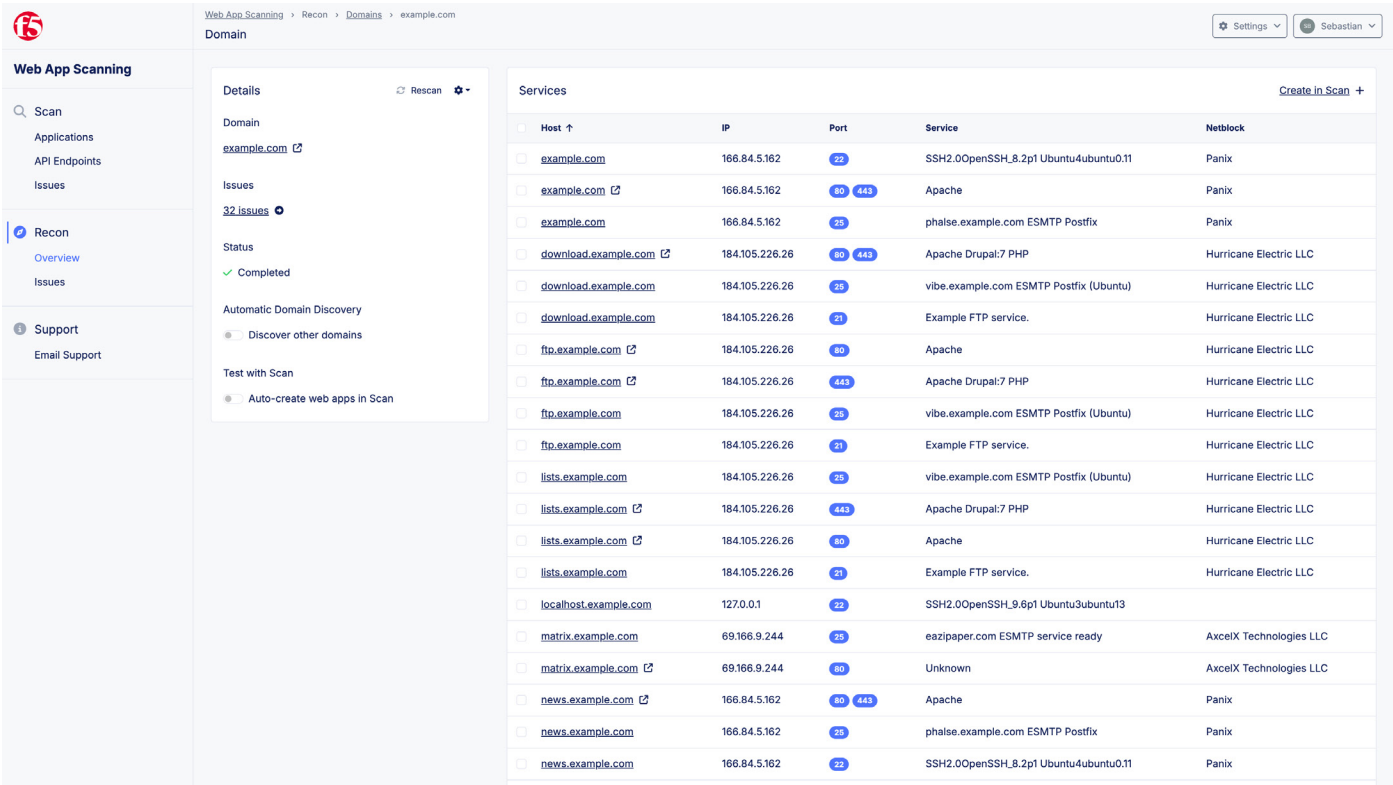


Figure 1: Gain a clear view of your web app’s external threat surface and any known vulnerabilities so corrective action can be taken.

Dynamic application security testing

Run automated tests against your organization’s web apps. Distributed Cloud Web App Scanning enables you to quickly and easily uncover vulnerabilities and determine how to safeguard your web apps from cyberthreats. Assess whether your apps are exposed to any of the risks outlined in the OWASP Top 10 for web applications and Top 10 for Large Language Model Applications, complete with in-depth—yet simple to understand—insights to help you mitigate threats. Additionally, Distributed Cloud Web App Scanning seamlessly integrates with F5 BIG-IP Advanced WAF, allowing you to import identified vulnerabilities for virtual patching through your BIG-IP Advanced WAF instances.

Embracing Distributed Cloud Web App Scanning mobilizes organizations with a proactive approach to navigating the ever-changing threat landscape.

Key features

Virtual patching

Integrates with F5 BIG-IP Advanced WAF so you can automatically import test results and apply signature sets to vulnerable endpoints in just a few clicks.

Comprehensive web app and API scanning

Crawls your domain(s), compiling a complete inventory of apps, APIs, services, exposed servers, known vulnerabilities, and potential leaked credentials.

Automated dynamic penetration testing

Automatically tests across web apps to uncover vulnerabilities and provide transparent results with visual evidence such as videos and screenshots of exploits.

Comprehensive and transparent reporting with AI support

Delivers detailed reporting with full context to simplify compliance and streamline issue resolution; AI assistants analyze vulnerabilities to provide technical insights and remediation guidance.

Continuous monitoring and scanning

Enable scheduled scans and tests of your app environment with notifications delivered via preferred channels.

Seamless integration with IT operations and DevOps tools

Supports various workflows with seamless integration into operations and CI/CD pipelines, including task tracking tools to boost visibility and accelerate update and remediation processes.

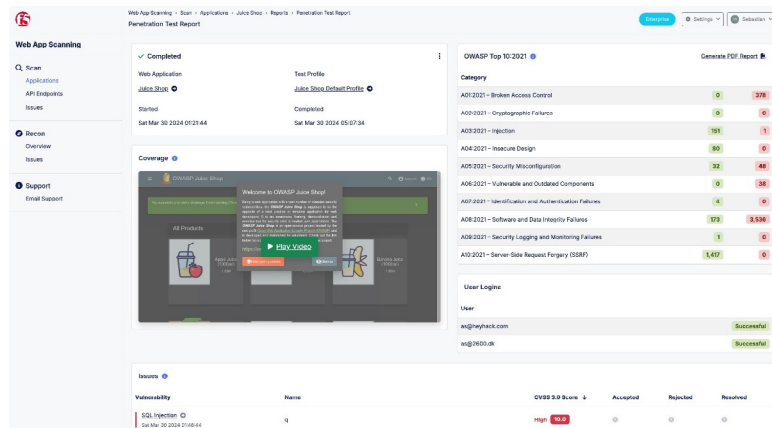


Figure 2: Set up tests in just a couple of clicks to quickly uncover unknown vulnerabilities, including risks outlined in the OWASP Top 10 for web applications and Top 10 for Large Language Model Applications, and learn how to safeguard your web apps from attack.

Distributed Cloud Web App Scanning is a cornerstone for web app and API security. It bridges the security gaps often left by infrequent pen testing cycles, delivering continuous visibility and actionable insights that empower organizations to fortify security and maintain compliance with critical standards as their app ecosystems continue to evolve.

Conclusion

As organizations increasingly leverage modern applications to drive innovation, they also face a wider array of security threats as dynamic as today's enterprise environments. Distributed Cloud Web App Scanning mobilizes organizations with a proactive approach to navigating this ever-changing threat landscape.

Distributed Cloud Web App Scanning provides effortless and continuous identification of critical infrastructure, services, and endpoints that make up an organization's web apps. Featuring one of the industry's most intuitive and comprehensive web app scanners, it automates the scanning process, generating deep and insightful analysis of potential vulnerabilities that aids in seamless response through virtual patching with surgical mitigations that stop attackers from exploiting specific vulnerabilities while ensuring web apps continue to perform for genuine users. By minimizing the attack surface and bolstering the security of the critical services and sensitive data that make up modern web apps, Distributed Cloud Web App Scanning ensures a robust defense against cyberthreats, safeguarding your digital assets while maintaining the integrity of your business.

To learn more, contact your F5 representative or visit f5.com/cloud/products/web-app-scanning.

